UNITED STATES DISTRICT COURT

for the

District of New Mexico

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

One cellular telephone seized from Tyler Witt and in the custody of the Bernalillo County Sheriff's Office

Case No. 24MR-922

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the _____ District of New Mexico, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 841	Distribution of a Controlled Substance
21 U.S.C. §846	Conspiracy to Distribute a Controlled Substance

The application is based on these facts:

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Gavin R. Hayes
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone *(specify reliable electronic means)*.

Date: May 13, 2024

Judge's signature

City and state: **Albuquerque, NM**

Laura Fashing, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF One cellular telephone seized from Tyler Witt and in the custody of the Bernalillo County Sheriff's Office	Case No. _____ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Gavin Hayes, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I, your affiant, make this affidavit in support of an application for a search warrant under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search a cellular telephone presently in the custody of the Bernalillo County Sheriff's Office (BCSO) that was seized from Tyler WITT. That cellular telephone is referred to herein as the "SUBJECT DEVICE" and further described and depicted in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations, hereafter referred to as HSI, and have been employed by HSI since August of 2023. I am currently assigned to the HSI office in Albuquerque, NM where I am assigned to investigate individuals involved in the trafficking of narcotics including violations of Title 21, United States Code, Section 841 and 846. I have worked narcotics investigations and has training in investigating these types of cases by the Department of Homeland Security and other governmental and non-governmental entities. During the investigation of these cases, I have participated in the execution of search warrants pertaining to these violations.

3. I have completed the Criminal Investigators Training Program (CITP) and Homeland Security Investigations Special Agent Training (HSISAT) at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. These training programs included topics such as constitutional law, customs and immigration law, civil and criminal forfeiture, narcotics investigations, financial investigations, physical and electronic evidence, investigative methods, and more.

4. Prior to my tenure as a Special Agent, I was a sworn law enforcement officer employed by the city of Greensboro, North Carolina. I served in this position for over 6 years, during which I was primarily assigned to the patrol bureau. My primary responsibilities were responding to 911 calls and investigating violations of criminal law. I investigated and assisted with investigating hundreds of felony and misdemeanor violent crimes, drug offenses, weapon violations, fraud offenses, impaired driving offenses, and more. I regularly established probable cause for warrantless arrests, arrest warrants, and search and seizure warrants for the aforementioned crimes.

5. My training as a Greensboro Police Officer included attending the Greensboro Police Academy, which included North Carolina's Basic Law Enforcement Training (BLET) program. Covered topics included constitutional law, criminal law, patrol duties, basic narcotics investigations, criminal investigations, basic interviewing, communication, and mental health awareness. Since completing the Greensboro Police Academy, I was certified by the State of North Carolina as a Chemical Analyst and as a Radar Operator. I received further specialized training in the areas of Fundamentals of the Investigative Process, Death and Violent Crime Scene Management, Standardized Field Sobriety Testing, Introduction to Drugged Driving, Drones for First Responders, and Roadside Interview and Detecting Deception.

6. Prior to my tenure as a Greensboro Police Officer, I received my education at Elon University in North Carolina. I received a Bachelor of Arts with majors in Public Health Studies and Policy Studies, and minors in Leadership Studies and Criminal Justice Studies.

7. In addition to my training and experience, I have developed information I believe to be reliable from additional sources including, but not limited to:

a. Information provided by Special Agents ("SA"), Criminal Analysts (CA) of the Department of Homeland Security, and other law enforcement officials ("Agents"), including oral and written reports that I have received directly or indirectly from said investigators;

b. Sources of Information (SOIs)

c. Results of physical surveillance conducted by agents during this investigation;

d. A review of telephone subscriber information;

e. A review of driver's license and automobile registration records;

f. Records from commercial databases;

g. Analysis of bank records and data seized from electronic devices; and

h. Records from the National Crime Information Center ("NCIC").

8. Because this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are relevant to the determination of probable cause to support the issuance of the requested warrant. When the statements of others are set forth in this Affidavit, they are set forth in substance and in part.

9. Based on the facts set forth in this Affidavit I believe there is probable cause that WITT has violated provisions of 21 U.S.C. § 841, Possession with Intent to Distribute a Controlled Substance, and 21 U.S.C. § 846, Conspiracy to Distribute a Controlled Substance. Your Affiant further submits that there is probable cause to believe that evidence and instrumentalities of those offenses are contained within the SUBJECT DEVICE.

10. The United States District Court for the District of New Mexico has jurisdiction to issue the proposed warrant because it is a "court of competent jurisdiction" as defined in 18 U.S.C. § 2711. Specifically, the Court has jurisdiction over federal criminal offenses in the District of New Mexico, *see* 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

11. In April of 2024, HSI agents in Phoenix, AZ, provided information to HSI Albuquerque SA Victor Avila. This information, from a Phoenix-based Source of Information (SOI), detailed that Matthew VALENZUELA and a subject known to the source only as "Tyler" were trafficking 150,000 fentanyl pills from Phoenix to Albuquerque. The SOI was able to provide a vehicle description of a newer white Toyota Camry with black rims. Law Enforcement database checks determined the vehicle would likely have a registration of New Mexico BLBA85. HSI Albuquerque agents attempted to interdict this delivery but were unsuccessful.

12. On May 2, 2024, SA Avila conducted surveillance at 1751 Bellamah Avenue NW in Albuquerque and located the Camry. SA Avila surveilled the vehicle and observed VALENZUELA leave the residence at that address carrying a trash bag, throw the trash bag in a dumpster, and depart the apartment in the Camry. SA Avila conducted a trash pull and located narcotic paraphernalia which tested positive for trace amounts of fentanyl. SA Avila also located a direct deposit information form with the name of "Tyler C Witt."

13. On May 9, 2024, at approximately 11:40 PM, detectives with the Bernalillo County Sheriff's Office (BCSO) conducted a traffic stop on a motorcycle at 1620 Indian School NW in Albuquerque. Detectives I. Dunbar and J. Mora initiated the traffic stop based on observations that the motorcycle did not have a displayed registration plate and that the operator (later identified as Tyler WITT) was attempting to start the motorcycle by manipulating wires on the motorcycle. Based on their training and experience, the Detectives believed that WITT was trying to start a stolen motorcycle

14. Detectives detained WITT and conducted routine records checks. They determined that WITT had an active warrant for his arrest out of Bernalillo County for Narcotics Trafficking. They searched WITT incident to his arrest.

a. During the search, the BCSO detectives located a black semiautomatic handgun in WITT's backpack. Further records checks indicated that WITT is a convicted felon, which restricted his rights to possess firearms.

b. The BCSO detectives also located a sandwich baggie in his front right pants pocket which contained a white powdery substance and M-30 blue pills. Based on the Detectives' training and experience, they recognized these substances to be cocaine and fentanyl pills.

c. The BCSO detectives also located and took custody of a cellular telephone, the SUBJECT DEVICE.

15. WITT was arrested by BCSO Detectives.

16. On May 10, 2024, HSI Special Agent Victor Avila and I interviewed WITT in custody at the Metropolitan Detention Center. Prior to the interview, SA Avila advised WITT of his Miranda Rights. WITT verbally waived his rights. During the interview, WITT admitted that

he both uses and sells narcotics. He admitted that he sells narcotics in order to support his own use.

17. Based on my training, experience, and research, I know that the cell phone is a wireless telephone with capabilities that allow it to function as digital cameras, portable media players, GPS navigation devices, and personal digital assistants (PDA). A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

18. Wireless telephones may also contain computer chips and memories that store vast amounts of information, including documents, records, photographs, and other data. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, smartphones, tablets, server computers, and network hardware. The term "digital media" includes personal digital assistants (PDAs),

smartphones, tablets, BlackBerry devices, iPhones, iPods, iPads, digital cameras, and cellular telephones. The term "storage media" includes any physical object upon which electronic data can be recorded, such as hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media or digital medium. Collectively, the terms "computer," "digital media," and "storage media" are referred to herein as "electronic media."

19. Additionally, wireless telephones may both be used to send and receive electronic communications over the internet and social media platforms. Those devices often retain such communications for indefinite periods.

20. Based on my training, experience, and participation in this and in similar investigations, I believe that individuals involved in illegal trafficking of controlled substances often keep evidence of their drug trafficking activities on their wireless telephones.

21. Drug traffickers often maintain records of their transactions in a manner similar to the record keeping procedures of legitimate businesses. Even after the drugs are sold, documentary records are often maintained for long periods of time, even years, to memorialize past transactions, the status of accounts receivable and accounts payable, and the names and telephone numbers of suppliers, customers, and co-conspirators. These records may be maintained in their wireless telephones. These records can reflect names, addresses and/or telephone numbers of associates and co-conspirators, the sale and purchase of controlled substances including precursors, customer lists, and amounts of money owed to the trafficker by customers and by the trafficker to his/her suppliers.

22. Other evidence of transportation, ordering, possession, and sale of drugs can include the following: telephone bills to show numbers called by the drug dealers (and hence potential associates), overnight mail receipts, bank statements, deposit and withdrawal slips,

savings books, investment statements, loan statements, other financial institution statements, and federal and state tax returns. This type of documentation can be stored on digital media and concealed on a wireless telephone.

23. The use of digital media, including smartphones, tablets, cellular phones, and digital devices, has become part of everyday life. This is also true for drug traffickers. Information stored in electronic form on all of the above-devices can provide evidence of drug trafficking. Drug traffickers frequently use some or all of these devices to communicate with co-conspirators, customers, sources of supply, and others involved in the drug trade. These communications include, but are not limited to, phone calls, text messages, SMS (Short Message Service) messaging, MMS (Multimedia Messaging Service) messaging, social media posts and messaging, and smartphone application messaging services. Smartphones, tablets, cellular phones, and digital devices are frequently capable of storing messages, emails, social media communications, and communications made over smartphone applications. The content of these communications will often provide evidence of drug trafficking. Numbers stored on a telephone (such as Caller ID lists reflecting recently received calls, speed dial lists of names and/or telephone numbers, and logs of outgoing and incoming calls) can provide evidence of who the drug dealer is calling, and thus the identity of potential associates.

24. Drug traffickers often take, or cause to be taken, photographs and/or videos of themselves, their associates, their property, and their drugs. They often maintain these photographs and/or videos in their wireless telephones and other digital devices. Smartphones, tablets, cellular phones, digital cameras, and other digital devices, often have the capability to take still photos and videos and save them indefinitely on the device's storage medium. Drug traffickers frequently use these devices to take their photographs and videos.

25. Documents and information showing who owns, occupies, or controls the device being searched may also show who is responsible for the information and evidence found on the SUBJECT DEVICE. Documents and items showing the identity of the persons owning, or controlling the device searched include, but are not limited to, utility and telephone bills, canceled envelopes and correspondence, outgoing answering machine messages, tax returns, keys, deeds, and mortgage receipts. In my training and experience, examining data stored on devices of this type can reveal relevant information and evidence of, among other things, evidence that reveals or suggests who possessed or used the device.

26. A list of items agents seek authority to seize is in Attachment B.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

27. As described above and in Attachment B, this application seeks permission to search for evidence and records that might be found on the SUBJECT DEVICE, in whatever form they are found. Much of the evidence and records described in the paragraphs above and in Attachment B can be produced and/or stored on electronic media. For this reason, I submit that there is probable cause to believe those records may be stored on the SUBJECT DEVICE. Thus, the warrant applied for would authorize the seizure of electronic media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

28. Necessity of seizing or copying entire electronic media: In most cases, a thorough search of the SUBJECT DEVICE for information that might be stored on electronic media often requires the seizure of the physical electronic media and later off-site review consistent with the warrant. In lieu of removing electronic media from the SUBJECT DEVICE, it is sometimes possible to make an image copy of electronic media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted

files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the electronic media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on the SUBJECT DEVICE could be unreasonable. Electronic media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the SUBJECT DEVICE. However, taking the electronic media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of electronic media formats that may require off-site reviewing with specialized forensic tools.

29. Nature of examination: Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying electronic media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the computer or entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

30. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock the device subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by

pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to

access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours and the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of without any identifying information on the exterior of the

device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found with the SUBJECT DEVICE and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual who was found with the SUBJECT DEVICE and is reasonably believed by law enforcement to be a user of the device to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

CONCLUSION

31. Based on the information and facts set forth in this affidavit, your Affiant submits that there is cause to believe that WITT possessed fentanyl with the intent to distribute it in violation of 21 U.S.C. § 841, and that he conspired with others to distribute fentanyl in violation of 21 U.S.C. § 846. Further, based upon the information contained herein, your Affiant submits that probable cause exists to believe that instrumentalities, fruits, and/or evidence of violations of 21 U.S.C. § 841 and 21 U.S.C. § 846 are located within the SUBJECT DEVICE further described in Attachment A.

32. WHEREFORE, your Affiant respectfully request that a warrant be issued authorizing Homeland Security Investigations, with appropriate assistance from other law enforcement officers, to search and examine the SUBJECT DEVICE for the information and evidence described in Attachment B.

AUSA Timothy Vasquez reviewed and approved this affidavit.

Respectfully submitted,

Gavin Hayes
Special Agent, HSI

Electronically submitted and telephonically sworn on May 13, 2024.

HONORABLE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

The property to be searched consist of one electronic device seized from the possession of Tyler WITT during his arrest on May 9, 2024, which is currently in the possession of the Bernalillo County Sheriff's Office. The device is further described as one cellular telephone, which is currently at the Metropolitan Detention Center, in the inventoried property of Tyler WITT. The device is specifically located at the MDC Warehouse "Property Room" in container 1618. The device is the only cellular telephone located in Tyler WITT's property.

ATTACHMENT B

ITEMS TO BE SEARCHED AND/OR SEIZED

All records, information, and evidence relating to violations of 21 U.S.C. § 841 and 21 U.S.C. § 846, including:

1. Data, communications, and information identifying co-conspirators and customers:
2. Data, communications, and information regarding the types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
3. Data, photos and videos of drugs, money, and or firearms;
4. Data, communications, and information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
5. Data, communications, and information regarding Tyler WITT's schedule or travel relating to the above offenses; and
6. Financial records or other information regarding the expenditure of disposition of proceeds from the distribution of controlled substances including all bank records, checks, credit card bills, account information, and other financial records.
7. Evidence of user attribution showing who used or owned the device at the time the things described in this warrant were created edited or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history:
8. Any information which conveys the identity or contact information of co-conspirators in the crimes being investigated.

As used above, the terms "data," "communications," "records," and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash

memory or other media that can store data), and photographic or video format, and any content within smartphone applications such as WhatsApp, Snapchat, Marco Polo, Facebook, Instagram, TikTok, Telegram, and others that are stored on the SUBJECT DEVICE.